北星論集(経) 第46巻 第2号（通巻第51号） March 2007

Setup of Windows Server 2003 and Networking with Active Directory in the Network Laboratory (I)

Hiroshi NOTO

Contents

1. Introduction
2. System Requirements and System Features
3. New Installation
 3.1. Licensing Mode
 3.2. Two Operating Systems
 3.3. File System for Installation Partition
 3.4. Disk Partitions or Volumes for New Installations
 3.5. Networks: TCP/IP, IP Addresses, Name Resolution
 3.6. Workgroups and Domains
4. Active Directory Overview
 4.1. Active Directory Server Roles
 4.2. Configuration of Domain Controllers
 4.3. Domain Name Service (DNS) Configuration
 4.4. Dynamic Host Configuration Protocol (DHCP)

Section 1. Introduction

We have planned to introduce and construct a business-to-business (B2B) integrated network system for the students in the Management and Information Department, Hokusei Gakuen University to understand and practice connecting applications, defining business processes, managing and monitoring business processes across the organization, and optimizing both internal and business-to-business processes. We implement our B2B network system in the Network Laboratory in the Comprehensive Information Center of our university.

In this article we are going to describe our network system, starting with introducing an operating system, selecting a server computer and installing the operating system on the server computer. We then explain how we set up the server system in detail. The main function of our server system is the Active Directory directory service that is configured to meet our B2B practice requirements.

Key Words: Windows Server 2003, Business-to-business(B2B) Integrated Network,
'Active Directory' Directory Service, Domain Controller,
Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP)

In Section 2 we describe the system requirements and the system features that enable the installation of an operating system Windows Server 2003[1), 2), 4)-6)]. In Section 3 the configuration of Windows Server 2003 is elaborated including licensing mode, two operating systems, file systems and partition, network connection and domain creation. In Section 4 we overview the Active Directory directory service[3)] and how to configure the Active Directory. We outline domain controllers, Domain Name Service (DNS) servers and Dynamic Host Configuration Protocol (DHCP) servers as well.

Installing applications which enable us to costruct the B2B network system will be explained in the forthcoming papers.

Section 2. System Requirements and System Features

We adopt Windows Server 2003, Enterprise Edition as the operating system on which we implement our network management system. The reason for choosing Windows Server 2003 is that it incorporates a set of Microsoft software technologies that enable software integration through the use of XML Web services. XML Web services are small reusable applications written in XML that allow data to be communicated between otherwise unconnected sources. And it is Windows Server 2003 that the server software we have planned to introduce requires as the operating system. We have to make sure that computers on which we install Windows Server 2003, Enterprise Edition meet some system requirements. To ensure adequate performance of the operating system the following requirements are to be satisfied for an x86-based computer (this is the case with our server computer):

1) One or more processors with a recommended minimum speed of 550 megahertz (MHz). The minimum supported speed is 133 MHz.

2) A maximum of eight processors per computer is supported. Processors from the Intel Pentium/Celeron family, AMD K6/Athlon/Duron family, or compatible processors are recommended.

3) 256 megabytes (MB) of RAM (recommended minimum). 128 MB is the minimum supported, and 32 gigabytes (GB) is the maximum supported.

4) For computers with more than 4 GB of RAM, hardware compatibility should be confirmed.

We prepare Dell PowerEdge 800 System as the server computer. The PowerEdge 800 is an excellent single-processor server for small businesses or remote offices. This server computer delivers good performance and availability features which are found in higher-end systems. PowerEdge 800 has the following system features:

- Processor:
  Intel Pentium 4 processor with an internal operating speed of at least 4.3 GHz (3.40 GHz, now), internal cache of (at least) 400 MB, and a front-side bus speed of at least 800 MHz.
- A minimum of 256 MB of 400-MHz or 533-MHz DDR 2 SDRAM memory, upgradable to a maximum of 4 GB by installing combinations of 256-MB, 512-MB, or 1-GB unbuffered ECC memory modules. At the moment 1.99 GB of RAM.
- Support for the following internal hard-drive configurations:
  Up to four internal, 1-inch, SATA hard drives with the integrated drive controller, or up to four SATA hard drives with the optional SATA RAID controller card.
  or
  Up to four internal, 1-inch, hot-pluggable (optional) SCSI hard drives with a SCSI controller card or SCSI RAID controller card.
- One 3.5-inch peripheral drive bay for the diskette drive, and two 5.25-inch bays for any combination of the following supported drives: CD, DVD, combination CD-RW/DVD, or tape backup unit.
- Support for hardware RAID using an optional SATA or SCSI RAID controller card.
- Support for external storage systems using an optional RAID controller card.
- Optional remote access card for remote systems management.
- Chassis intrusion alarm and a bezel lock that prevents access to the hard drives.
- The system board includes the following features:
  -Single integrated drive controller that supports up to four SATA hard drives and one IDE CD, DVD, or CD-RW/DVD combination drive, and an IDE tape backup unit.
  -Five PCI slots: two PCI Express x1 (3.3 V) slots, two 64-bit, 100-MHz PCI-X (3.3 V) slots, and one 32-bit, 33-MHz PCI (5 V) slot.
- An integrated Gigabit Ethernet NIC, capable of supporting 10-Mbps, 100-Mbps, or 1000-Mbps data rates, with support for PXE and Wake-on-LAN.
- Four USB 2.0-compliant connectors (two on the front and two on the back) capable of supporting a diskette drive, a CD-ROM drive, a keyboard, a mouse, or a USB flash drive.
- An integrated SVGA-compatible video subsystem with an Intel MCH video controller. This video subsystem shares 8 MB of SDRAM system memory (nonupgradable). True-color graphics are supported in the following resolutions: 640 x 480, 800 x 600, 1024 x 768, and 1280 x 1024.
- Systems management circuitry that monitors critical system voltages and fan speeds. The systems management circuitry works in conjunction with the systems management software.
- Standard baseboard management controller with serial access.
- Back-panel connectors include mouse, keyboard, serial, video, parallel, two USB connectors, and a NIC connector.
- Front-panel connectors include two USB connectors.

Section 3. New Installation

3.1. Licensing Mode

Products in the Windows Server 2003 family support two licensing modes:

Per Device or Per User and **Per Server**. In the **Per Device or Per User** mode, each device or user that accesses a server running a product in the Windows Server 2003 family requires a separate Client Access License (CAL). With one CAL, a particular device or user can connect to any number of servers running the Windows Server 2003 family. This is the most commonly used licensing method for companies with more than one server running the Windows Server 2003 family. In contrast, **Per Server** licensing means that each concurrent connection to this server requires a separate CAL. In other words, this server can support a fixed number of connections at any one time. For example, if we select the Per Server client-licensing mode with five licenses, this server could have five concurrent connections at any one time (if each client requires one connection, this is five clients at any one time). The clients using the connections do not need any additional licenses.

The Per Server licensing mode, therefore, is often preferred by small companies or organizations like ours with only one server. It is also useful for Internet or remote access servers where the client computers might not be licensed as network clients for products in the Windows Server 2003 family. We can specify a maximum number of concurrent server connections and reject any additional logon requests. If we are unsure which mode to use, we choose **Per Server**, because we can change once from Per Server mode to Per Device or Per User mode at no cost. In the present case we select Per Server licensing mode.

3.2. Two Operating Systems

3.2.1. Multiple Operating Systems

On a computer with an appropriate disk configuration, we can install more than one operating system, and then choose between the operating systems each time we restart the computer. For example, on an x86-based computer, we could set up a server to run Windows Server 2003, Enterprise Edition, most of the time, but allow it to sometimes run Windows Server 2000, Standard Edition, to support an older application. During restarts, a display appears for a specified number of seconds, allowing us to select between the two operating systems. (We can specify a default operating system that will run if no selection is made during the restart process.)

The disk configurations consist of the basic disks and the dynamic disks on which we install more than one operating system (see 3.4). On a basic disk, we must install each operating system in a separate partition. This ensures that each operating system does not overwrite crucial files that are needed by another operating system. Windows Server 2003 family initially installs the operating system using a basic disk format.

3.2.2. Multiple Partitions with Products in Windows Server 2003 Family

On computers that contain multiple partitions with products in the Windows Server 2003 family, we can install each operating system on a different partition, and install the applications used with an operating system on the same disk or partition with it. If an application is used with two different operating systems, install it in two places. For an x86-based computer, we can choose any product in the Windows Server 2003 family for installation on a specific partition. If the computer participates in a domain (see 3.6), we use a different computer name for each installation. Because a unique security identifier (SID) is used for each installation on a domain, the computer name for each installation must be unique, even for multiple installations on the same computer.

We have planned to install Windows Server 2003 in English and Windows Server 2003 in Japanese on the same computer, Dell PowerEdge 800.

3.3. File System for Installation Partition

On computers that contain multiple operating systems, compatibility becomes more complex when we consider file system choices. The file systems to choose from are NTFS, FAT, and FAT32. We must choose among three file systems for an installation partition.

3.3.1. File System Compatibility

NTFS is normally the recommended file system because it is more efficient and reliable, and supports important features including Active Directory and domain-based security. With NTFS, however, we need to take file system compatibility into account when considering whether to set up a computer to contain more than one operating system, because with Windows 2000 and the Windows Server 2003 family, NTFS has new features in addition to those in Windows NT. Files that use any new features will be completely usable or readable only when the computer is started with Windows 2000 or a product in the Windows Server 2003 family. For example, a file that uses the new encryption feature will not be readable when the computer is started with Windows NT Server 4.0 or Windows NT Server 4.0, Enterprise Edition, which were released before the encryption feature existed.

When we format a partition during Setup, the file systems we can choose are listed as NTFS and FAT in Table 1 which provides information about the relationship between partition size and file system choices during Setup.

Table 1. The relationship between partition size and file system choices during Setup.

State and size of partition	Setup choices and responses (when formatting the partition)
Unformatted, less than 2 GB.	Setup offers NTFS or FAT. Setup uses the format chosen.
Unformatted, 2 GB or larger, up to a maximum of 32 GB.	Setup offers NTFS or FAT. If FAT is chosen, Setup uses FAT32.
Unformatted, larger than 32 GB.	Setup allows only NTFS.

If we format a partition during Setup, we can choose between a quick format and a full format:

Quick format A quick format creates the file system structure on the disk without verifying the integrity of every sector. We choose this method for any disk that has no bad sectors and no history of file-corruption problems that might be related to bad sectors.
Full format A full format identifies and tracks bad sectors so that they are not used for storing data. We choose this method for any disk that has bad sectors or has a history of file-corruption problems that might be related to bad sectors.

In our case we adopt the NTFS file system and we select a full format.

3.3.2. NTFS compared to FAT and FAT32

We go into NTFS in detail compared to FAT and FAT32. NTFS has always been a more powerful file system than FAT and FAT32. Windows 2000, Windows XP, and the Windows Server 2003 family include a new version of NTFS, with support for a variety of features including Active Directory, which is needed for domains, user accounts, and other important security features. FAT and FAT32 are similar to each other, except that FAT32 is designed for larger disks than FAT. The file system that works most easily with large disks is NTFS.

Table 2 describes the compatibility of each file system with products in the Windows Server 2003 family and compares disk and file sizes possible with each file system.

Table 2. Comparisons between disk and file sizes possible with each file system.

NTFS	FAT	FAT32
Recommended minimum volume size is approximately 10 MB. Maximum volume and partition sizes start at 2 terabytes (TB) and range upward. For example, a dynamic disk formatted with a standard allocation unit size (4 KB) can have partitions of 16 TB minus 4 KB. Cannot be used on floppy disks.	Volumes from floppy disk size up to 4 GB. Does not support domains.	Volumes from 33 MB to 2 TB can be written to or read using products in the Windows Server 2003 family. Volumes up to 32 GB can be formatted as FAT32 using products in the Windows Server 2003 family. Does not support domains.
Maximum file size is potentially 16 TB minus 64 KB, although files cannot be larger than the volume or partition they are located on.	Maximum file size is 2 GB.	Maximum file size is 4 GB.

3.3.3. Features available with NTFS

This section provides background information about the features available with NTFS. Some of these features include:

• Better scalability to large drives. The maximum partition or volume size for NTFS is

much greater than that for FAT, and as volume or partition sizes increase, performance with NTFS does not degrade as it does with FAT.

- Active Directory (and domains, which are part of Active Directory). With Active Directory, we can view and control network resources easily. With domains, we can fine-tune security options while keeping administration simple. Domain controllers and Active Directory require NTFS.
- Compression features, including the ability to compress or uncompress a drive, a folder, or a specific file. (However, a file cannot be both compressed and encrypted at the same time.)
- File encryption, which greatly enhances security. (However, a file cannot be both compressed and encrypted at the same time.)
- Permissions that can be set on individual files rather than just folders.
- Remote Storage, which provides an extension to our disk space by making removable media such as tapes more accessible.
- Recovery logging of disk activities, which allows NTFS to restore information quickly in the event of power failure or other system problems.
- Sparse files. These are very large files created by applications in such a way that only limited disk space is needed. That is, NTFS allocates disk space only to the portions of a file that are written to.
- Disk quotas, which we can use to monitor and control the amount of disk space used by individual users.

3.4. Disk Partitions or Volumes for New Installations

As already stated before, there are two disk storage types, basic and dynamic supported in Windows Server 2003. The underlying difference between the two is the use of partitions versus volumes for disk management. Both are physical disks, but the basic type contains partitions, extended partitions, logical drives and an assortment of static volumes; the dynamic type does not use partitions but dynamically manages volumes and provides advanced storage options.

Partitions are divisions of physical space on the same disk. Volume can consist of one or more disks or portions of them and must be of the same storage type. Windows Server 2003 initially installs the operating system using a basic disk format. Although the basic format works well, an upgrade to a dynamic disk is required to create spanned, striped, mirrored, or RAID-5 volumes.

We must plan our disk partitions before we run Setup only if both of the following conditions are true:

- We are performing a new installation, not an upgrade.
- The disk on which we are installing is a basic disk, not a dynamic disk. Basic disks are the disk type that existed before Windows 2000; most disks are basic disks.

Disk partitioning is a way of dividing our physical disk so that each section functions as a separate unit. When we create partitions on a basic disk, we divide the disk into one or more areas that can be formatted for use by a file system, such as FAT or NTFS. Different partitions often have different drive letters (for example, C: and D:). A basic disk can have up to four primary partitions, or three primary partitions and one extended partition. (An extended partition can be subdivided into logical drives, while a primary partition cannot be subdivided.)

Before we run Setup to perform a new installation, we determine the size of the partition on which to install. There is no set formula for figuring a partition size. The basic principle is to allow plenty of room for the operating system, applications, and other files that we plan to put on the installation partition. The files for setting up Windows Server 2003, Enterprise Edition, require approximately 2 GB to 3 GB on an x86-based computer. It is recommended that we allow considerably more disk space than the minimum amount. It is not unreasonable to allow 4-40 GB on the partition, or more for large installations. This allows space for a variety of items, including optional components, user accounts, Active Directory information, logs, future service packs, the paging file used by the operating system, and other items.

In many cases we create and size only the partition on which we want to install Windows Server 2003, Enterprise Edition during Setup. After installation is complete, we can use Disk Management to manage new and existing disks and volumes. This includes creating new partitions from unpartitioned space; deleting, renaming, and reformatting existing partitions; adding and removing hard disks; and changing a basic disk to the dynamic.

3.4.1. Option of Disk Partition

We can change the partitions on our disk during Setup only if we are performing a new installation, not an upgrade. We can modify the partitioning of the disk after Setup by using Disk Management. Setup examines the hard disk to determine its existing configuration, and then offers the following options:

- If the hard disk is unpartitioned, we can create and size the partition on which you will install the Windows Server 2003 family.
- If the hard disk is partitioned but has enough unpartitioned disk space, we can create the partition for our Windows Server 2003 family product by using the unpartitioned space.
- If the hard disk has an existing partition that is large enough, we can install a product in the Windows Server 2003 family on that partition, with or without reformatting the partition first. Reformatting a partition erases all data on the partition. If we do not reformat the partition where there is already an operating system, but we do install a Windows Server 2003 family product, that operating system will be overwritten, and we

must reinstall any applications we want to use with the Windows Server 2003 family product.

- If the hard disk has an existing partition, we can delete it to create more unpartitioned disk space for a partition for a Windows Server 2003 family product. Deleting an existing partition also erases any data on that partition.

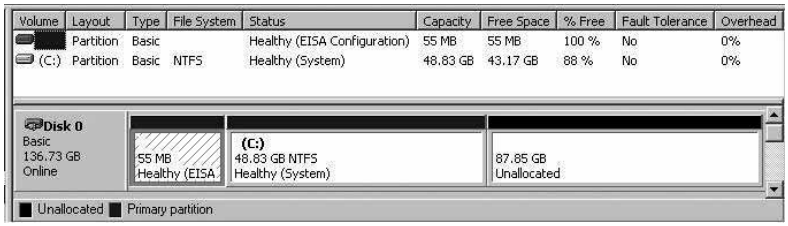

Figure 1. The disk partition on PowerEdge 800.

We show in Figure 1 how the disk on our server computer is partitioned. We divide the disk to two partitions, one of which called C: drive we allocate 48.83 GB on.

3.5. Networks: TCP/IP, IP Addresses, Name Resolution

TCP/IP is the network protocol that provides Internet access. It is the protocol used by most servers, although we can use additional or different network adapters and their associated protocols on our servers. Setup and "Manage Your Server" (which includes the Configure Your Server Wizard) after Setup is finished are designed to make it easy to configure TCP/IP and the services that support it.

To use TCP/IP, we make sure that each server is provided with an IP address, either a dynamic or automatic address provided through software, or a static address that we obtain from the system administrator in the computing center. Because these addresses are numbers and therefore hard to remember, we will also have to provide users with names that are easier to use. Mapping this type of name to an IP address is called name resolution, and can be accomplished by various methods, primarily the Domain Name System (DNS) and Windows Internet Name Service (WINS).

As outlined in the preceding paragraph, using TCP/IP requires that an IP address be provided for each computer. The next subsection describes the DNS service.

3.5.1. Domain Name System (DNS)

Name resolution is a process that provides users with easy-to-remember server names, instead of requiring them to use the numerical IP addresses by which servers identify themselves on the TCP/IP network. The name-resolution services are Domain Name System (DNS) and Windows Internet Name Service (WINS). WINS is the name resolution system used for WindowsNT Server 4.0 and earlier operating system.

DNS is a hierarchical naming system used for locating computers on the Internet and

private TCP/IP networks. One or more DNS servers are needed in most installations. DNS is required for Internet e-mail, Web browsing, and Active Directory. DNS is often used as a name resolution service in domains with clients running the Windows Server 2003 family.

DNS is installed automatically when we create a domain controller (or when we install Active Directory on an existing member server, which makes it a domain controller), unless the software for Windows Server 2003, Enterprise Edition detects that a DNS server already exists for that domain. We can also install DNS by choosing the DNS server role in "Manage Your Server" or by using "Add/Remove Windows Components", which is part of Add or Remove Programs in Control Panel.

If we plan to install DNS on a server, we specify a static IP address on that server and configure that server to use that IP address for its own name resolution. Figure 2 shows the internet protocol (TCP/IP) properties where we specify the IP address of the server computer, along with the default gateway address and the preferred DNS server address given from our Comprehensive Information Center.

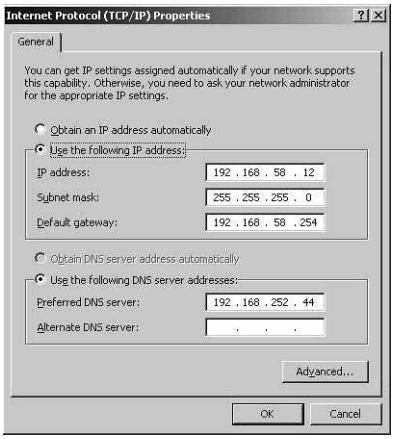

Figure 2. Internet protocol (TCP/IP) properties.

3.6. Workgroups and Domains

A *domain* is a group of accounts and network resources that share a common directory database and set of security policies, and might have security relationships with other domains. A *workgroup* is a more basic grouping, intended only to help users find objects such as printers and shared folders within that group. Domains are the recommended choice for all networks except very small ones with few users.

In a workgroup, users might have to remember multiple passwords, one for each network resource. (In addition, different users can use different passwords for each resource.) In a domain, passwords and permissions are simpler to keep track of, because a domain has a single, centralized database of user accounts, permissions, and other network details. The information in this database is replicated automatically among domain controllers. We determine which servers are domain controllers and which are simply members of the domain (see

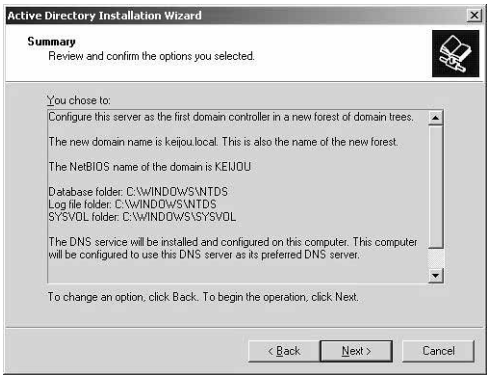

Figure 3. Summary of Active Directory installation.

the next subsection). We can determine these roles not only during Setup but afterward. We specify a name "keijou.local" for our new domain in our Network Laboratory (Figure 3).

Domains and the Active Directory directory system of which domains are a part, provide many options for making resources easily available to users while maintaining good monitoring and security.

3.6.1. Plan for Domain Controllers and Member Servers

With Windows Server 2003, Enterprise Edition, servers in a domain can have one of two roles: *domain controllers* and *member servers*. Domain controllers contain matching copies of the user accounts and other Active Directory data in a given domain. Member servers belong to a domain but do not contain a copy of the Active Directory data. (A server that belongs to a workgroup, not a domain, is called a *stand-alone server*.) It is possible to change the role of a server back and forth from domain controller to member server (or stand-alone server), even after Setup is complete. However, it is recommended that we plan our domain before running Setup and change server roles (and server names) only when necessary.

Our Windows Server 2003, Enterprise Edition server plays the role of the domain controller in the domain "keijou.local".

4. Active Directory Overview

A directory is a hierarchical structure that stores information about objects on the network. A directory service provides the methods for storing directory data and making this data available to network users and administrators. Active Directory[3] is an implementation of LDAP[7] directory services by Microsoft for use in Windows environments (e.g. Windows Server 2003). Active Directory (abbreviated as AD) is a directory service used to store information about the network objects across a domain. The network objects fall into three broad categories — resources (e.g. servers, volumes and printers), services (e.g. e-mail), and users (accounts and passwords or users and groups). The AD provides information on the objects, organizes the objects, controls access, and sets security.

We install the Active Directory directory service on Microsoft Windows Server 2003, Enterprise Edition.

Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network. Policy-based administration eases the management of even the most complex network.

4.1. Active Directory Server Roles

As already described, computers that function as servers within a domain can have one

of two roles: member server or domain controller. A server that is not in a domain is a stand-alone server.

4.1.1. Member Servers

A member server is a computer that runs an operating system in the Windows 2000 Server family or the Windows Server 2003 family, that belongs to a domain, and that is not a domain controller.

A member server does not process account logons, participate in Active Directory replication (see the next subsection), or store domain security policy information. The security-related features are group policy, access control, user rights and security account database.

Member servers typically function as the following types of servers: file servers, application servers, database servers, Web servers, certificate servers, firewalls, and remote access servers.

4.1.2. Domain Controllers

A domain controller is a computer that:

- Runs an operating system in the Windows 2000 Server family or the Windows Server 2003 family.
- Uses Active Directory to store a read-write copy of the domain database, participate in multimaster replication, and authenticate users.

Domain controllers store directory data and manage communication between users and domains, including user logon processes, authentication, and directory searches. Domain controllers synchronize directory data using multimaster replication, ensuring consistency of information over time. Active Directory supports multimaster replication of directory data between all domain controllers in a domain.

The Active Directory database is replicated between domain controllers. The data replicated between controllers called "data" are also called "naming context". Only the changes are replicated, once a domain controller has been established. Active Directory uses a multimaster replication which means changes can be made on any controller and the changes are sent to all other controllers. The replication path in Active Directory forms a ring which adds reliability to the replication. Domain controllers, therefore, each contain a "replica" which is a copy of the domain directory.

As the needs of our computing environment change, we might want to change the role of a server. Using the Active Directory Installation Wizard, we can install Active Directory on a member server to make it a domain controller, or you can remove Active Directory from a domain controller to make it a member server.

We use our Windows Server 2003 as our domain controller. When we create the first

domain controller in our Network Laboratory, we are also creating the first domain, the first forest, the first site, and installing Active Directory. (As for "forest" and "site", see the next subsection.) Domain controllers running Windows Server 2003 store directory data and manage user and domain interactions, including user logon processes, authentication, and directory searches.

In a small organization, like our Network Laboratory using a single local area network (LAN), it is often a good practice to make one domain and to put at least one domain controller. A larger organization with many network locations will need one or more domain controllers in each site to provide high availability and fault tolerance to enhance network performance.

When users log on to the network, a domain controller must be contacted as part of the logon process. If clients must connect to a domain controller located in a different site, the logon process can take a long time. By creating a domain controller in each site, user logons are processed more efficiently within the site.

4.2. Configuration of Domain Controllers

Domains are units of replication. All of the domain controllers in a particular domain can receive changes and replicate those changes to all other domain controllers in the domain. Each domain in Active Directory is identified by a Domain Name System (DNS) domain name and requires one or more domain controllers. If our network requires more than one domain, we can easily create multiple domains. One or more domains that share a common schema and global catalog are referred to as a "forest". The first domain in a forest is referred to as the forest root domain. A single domain can span multiple physical locations or "sites" and can contain millions of objects. Site structure and domain structure are separate and flexible. A single domain can span multiple geographical sites, and a single site can include users and computers belonging to multiple domains.

4.2.1. Organizational Units

A domain defines a scope or unit of policy. A Group Policy object (GPO) establishes how domain resources can be accessed, configured, and used. These policies are applied only within the domain and not across domains. Each domain has its own security policies and trust relationships with other domains. The forest is the final security boundary.

In our case, we create one domain which spans one site and require one domain controller. We do not need to create separate domains merely to reflect our organization of divisions and departments. Within a domain, we can use organizational units for this purpose. Using organizational units helps us manage the accounts and resources in the domain. We can then assign Group Policy settings and place users, groups, and computers into the organizational units. Using a single domain greatly simplifies administrative overhead.

4.2.2. Domain Creation

We establish a domain by creating the first domain controller for a domain. To do this, we install Active Directory on a member server running Windows Server 2003 by using the Active Directory Installation Wizard. The wizard uses the information that we provide to create the domain controller and create the domain within the existing domain structure of our Network Laboratory. Depending on the existing domain structure, the new domain could be the first domain in a new forest, the first domain in a new domain tree, or a child domain of an existing domain tree.

A domain controller provides the Active Directory directory service to network users and computers, stores directory data, and manages user and domain interactions, including user logon processes, authentication, and directory searches. Every domain must contain at least one domain controller.

After we create the first domain controller for a domain, we can create additional domain controllers, if necessary, in an existing domain for fault tolerance and high availability of the directory.

4.3. Domain Name Service (DNS) Configuration

By default, the Active Directory Installation Wizard attempts to locate an authoritative DNS server for the new domain from its list of configured DNS servers that will accept a dynamic update of a service (SRV) resource record. If found, all the appropriate records for the domain controller are automatically registered with the DNS server after the domain controller is restarted.

If a DNS server that can accept dynamic updates is not found, either because the DNS server does not support dynamic updates or dynamic updates are not enabled for the domain, then the Active Directory Installation Wizard will take the following steps to ensure that the installation process is completed with the necessary registration of the SRV resource records:

1. The DNS service is installed on the domain controller and is automatically configured with a zone based on the Active Directory domain.

   For example, if the domain that we chose for our first domain in the forest is "keijou.local", then a zone rooted at the DNS domain name of "keijou.local" is added and configured to use the DNS Server service on the new domain controller.

2. A text file containing the appropriate DNS resource records for the domain controller is created.

   The file called Netlogon.dns is created in the systemroot\System32\Config folder and contains all the records needed to register the resource records of the domain controller. Netlogon.dns is used by the Net Logon service and supports Active Directory on servers running non-Windows Server 2003 DNS. In our case we have

Netlogon.dns records in the C:¥WINDOWS¥system32¥config folder.

If no DNS servers are available on the network, we can choose the option to automatically install and configure a local DNS server when we install Active Directory using the Active Directory Installation Wizard. The DNS server will be installed on the server on which we are running the wizard, and the server's preferred DNS server setting will be configured to use the new local DNS server.

Before running the Active Directory Installation Wizard, we ensure that the authoritative DNS zone allows dynamic updates and that the DNS server hosting the zone supports the DNS SRV resource record.

4.4. Dynamic Host Configuration Protocol (DHCP)

As outlined in the preceding section, using TCP/IP requires that an IP address be provided for each computer. There are two basic approaches for providing an IP address for a server we are installing:

4.4.1. DHCP Server

We can provide IP addresses to the computers on our network by configuring one or more DHCP servers, which provide IP addresses dynamically to other computers. A DHCP server must itself be assigned a static IP address.

One server or several servers can provide DHCP along with one or more name resolution services, which are called Domain Name System (DNS) and Windows Internet Name Service (WINS).

If we want to run Setup before we have finalized our decisions about which server to use as our DHCP server and what static IP address to assign to that server, we can choose Typical settings in the Networking Settings dialog box during Setup and complete the network configuration later. If we do this and there is no DHCP server in the network, Setup will use a limited IP addressing option called Automatic Private IP Addressing (APIPA)[8]. During the time that a server is using APIPA, it can communicate only with other computers using APIPA on the same network segment. A server that is using APIPA cannot make connections to the Internet (for browsing or email), and cannot be used with DNS or Active Directory (which depends on DNS).

If we know which server we want to use as our DHCP server, when installing that server, in the Networking Settings dialog box in Setup, we choose Custom settings, and specify a static IP address and related network settings.

4.4.2. Static IP Address

For certain types of servers, we must assign a static IP address and subnet mask during or after Setup. This is the case with our Windows Server 2003 in the Network Laboratory. These servers include DHCP servers, DNS servers, WINS servers, and any server providing

access to users on the Internet. It is also recommended that we assign a static IP address and subnet mask for each domain controller. If a computer has more than one network adapter, we must assign a separate IP address for each adapter.

4.4.3. DHCP Definition

Dynamic Host Configuration Protocol (DHCP) is an IP standard for simplifying management of host IP configuration. The DHCP standard provides for the use of DHCP servers as a way to manage dynamic allocation of IP addresses and other related configuration details for DHCP-enabled clients on our network.

Every computer on a TCP/IP network must have a unique IP address. The IP address (together with its related subnet mask) identifies both the host computer and the subnet to which it is attached. When we move a computer to a different subnet, the IP address must be changed. DHCP allows us to dynamically assign an IP address to a client from a DHCP server IP address database on our local network: for TCP/IP-based networks, DHCP reduces the complexity and amount of administrative work involved in reconfiguring computers.

As is explained in the previous sections, we have planned to configure DNS server and DHCP server on the same server computer which has a static IP address.

The server computer running a Windows Server 2003 operating system, therefore, is configured as a DHCP server for the local subnet. This server computer must contain and manage scope and other address-configurable information for the local subnet it serves. In Figure 4, we finally show that a DNS sever and a DHCP sever are configured and both servers are running successfully.

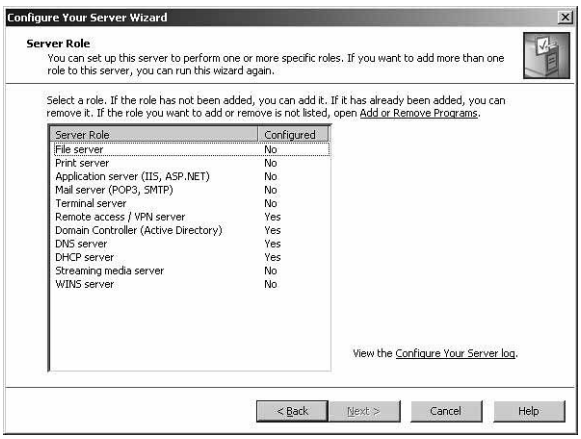

Figure 4. The configuration of our server is summarized.

Acknowledgements

The present research was supported by the Special Research Funds 2005 of Hokusei Gakuen University. The network configuration was carried out on Microsoft Windows Server 2003 operating system using Dell PowerEdge 800 computer in the Network Laboratory in the Comprehensive Information Center of Hokusei Gakuen University.

Bibliography

(1) Robert Williams and Mark Walla: The Ultimate Windows Server 2003 System Administrator's Guide (2003), Addison-Wesley.
(2) Windows Server 2003R2 Enterprise Edition system disk (2006) in MSDN Library.
(3) Active Directory:
http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/activedirectory/default.mspx
(4) Windows Server 2003 R2: http://www.microsoft.com/windowsserver2003/default.mspx
(5) Amano Tukasa: Windows Server 2003 at a Glance (Official Guide Book of Microsoft) (2003), Nikkei BP Soft Press (in Japanese)
(6) Inoue Koji: Windows Server 2003 Network Server Build Guide (2003), Shuwa System.
(7) In computer networking, the Lightweight Directory Access Protocol, or LDAP ("ell-dap"), is a networking protocol for querying and modifying directory services running over TCP/IP.
(8) Automatic Private IP Addressing (APIPA)
A TCP/IP feature in Windows XP and Windows Server 2003 that automatically configures a unique IP address from the range 169.254.0.1 through 169.254.255.254 with a subnet mask of 255.255.0.0 when the TCP/IP protocol is configured for automatic addressing, the Automatic private IP address alternate configuration setting is selected, and a DHCP server is not available. The APIPA range of IP addresses is reserved by the Internet Assigned Numbers Authority (IANA) for use on a single subnet, and IP addresses within this range are not used on the Internet.

[Abstract]

Setup of Windows Server 2003 and Networking with Active Directory in the Network Laboratory (I)

Hirosi NOTO

We have planned to introduce and configure a business-to business (B2B) integrated network system for the students in the Management and Information Department of Hokusei Gakuen University to help them understand and practice connecting applications, defining business processes, managing and monitoring business processes across the organization, and optimizing both internal and B2B processes. This B2B network system will be set up in the Network Laboratory in the Comprehensive Information Center of this university. This article describes the network system, starting with the introduction of an operating system (Windows Server 2003) and the selection of a server computer. It also describes how to install the operating system on the server computer. The article explains in detail how to set up the server system. The main component of the server system is the Active Directory directory service that is configured to meet the B2B practice requirements on Windows Server 2003. The configuration of Windows Server 2003 is fully elaborated, including licensing mode, two operating systems, file systems and partition, network connections and domain creation. The Active Directory directory service and how to establish it, configuring domain controllers, Domain Name Service (DNS) configuration, and Domain Host Configuration Protocol (DHCP) are also explained.

Key Words: Windows Server 2003, Business-to-business(B2B) Integrated Network
'Active Directory' Directory Service, Domain Controller
Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP)